GDPR – международный закон, новый регламент, нацеленный на «законное» хранение и обработку персональных данных жителей ЕС. Распространяется на компании, которые прямым или косвенным образом получают персональные данные физических лиц, позволяющих идентифицировать человека, выделить его из «толпы». Данный закон нацелен на защиту данных, гарантируя физическому лицу безопасность. Хотя на практике, это не совсем так. Разница лишь в том, что с появлением GDPR компании обязаны получить согласие, на обработку и хранения персональных данных, при этом в необъятном текстовом документе должно быть указано: зачем компании эти данные, и как долго они должны храниться на ресурсе. По-хорошему, компания должна сократить длительность хранения данных, исключить те данные, которые не являются необходимостью. Однако, учитывая, что данные всё же хранятся определенное время, этого достаточно, чтоб использовать данные идентификации для выявления поведенческих паттернов, используя анализ полученной информации для коммерческих целей. Таким образом, все компании, которые как-либо взаимодействуют и физическими лицами, являющимися гражданами ЕС, должны привести свои дела в порядок, соблюдая ряд необходимых изменений, учитывая все 99 статей регламента GDPR.  
С точки зрения компаний, вводятся два понятия: контроллер и процессор. Контроллер данные собирает, а процессор – обрабатывает. Но контроллер несет большую часть ответственности, заключают с процессорами соглашения о соблюдении правил регламента при обработке переданных данных. Компания должна четко и доступно донести пользователю, какие конкретно данные они собирают, и зачем это надо. Закон считается нарушенным сразу, как только было выявлено малейшее несоответствие в запрашиваемом и предоставляемом. А данные оплошности сулят колоссальными штрафами – 4% годовой прибыли или 20млн евро. Не считая потери репутации в глазах своих клиентов. Также закон обязывает контроллера обезличивать данные и хранить их в разных местах, что гарантирует безопасность персональных данных. Процессор обязан иметь протоколы доступа к данным. Если их нет, в случае утечки комиссия выявляет нарушения, награждая компании вышеописанными штрафами. Так что же должны сделать компании, в соответствии с новым регламентом? В первую очередь – проанализировать, в каком состоянии находятся сбор и обработка данных в текущий момент. Если на сегодняшний день используется один сервер, который в теории (да и на практике) можно взломать, необходимо разделить данные на несколько серверов. Даже если взломают один – сложно будет собрать «пазл», так как данные разбиты на несколько серверов. По принципу «не храните яйца в одной корзине». Также правильным решением будет разделить каналы передачи данных, а в случае утечки оперативно выявить и отключить один из каналов, а по другому каналу произвести необходимые работы по устранению неполадок. Таким образом, если компания обеспечивает сохранность, соблюдает регламент, не использует данные для продажи коммерческим организациям и содержит в своем штате сотрудников, регулярно занимающихся мониторингом вопросов, связанных с персональными данными – могут смело работать, не опасаясь многомиллионных штрафов, а также потери репутации и судебных тяжб